Elektrobit

UDACITY

Functional Safety Concept: Lane Assistance

Document version: 0.1

Template version: 1.0, Released on 2017-06-21

Author:
Konstantin Selyunin

August 26, 2018

Revision History

Version	Date	Editor	Description
0.1	2018/08/23	Konstantin Selyunin	LaTeX template created
0.2	2018/08/23	Konstantin Selyunin	Filling the content part

Contents

1 Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to look at the general functionality of the lane assistance item and define the functional safety requirements. It is also worth noting that the functional requirements definition should be done at a higher abstraction level, without going deep into technical details. According to the ISO 26262 [1] these functional safety requirements will then be refined to the technical safety requirements.

2 Inputs to the Functional Safety Concept

2.1 Safety goals from the Hazard Analysis and Risk Assessment

The safety goals for the lane assistance item are presented in Table 21

Table 21: Safety Goals

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

2.2 Preliminary Architecture

The preliminary architecture of the lane assistance item is shown in Figure 21.

2.2.1 Description of architecture elements

The functional description of the architecture elements is shown in Table 22.

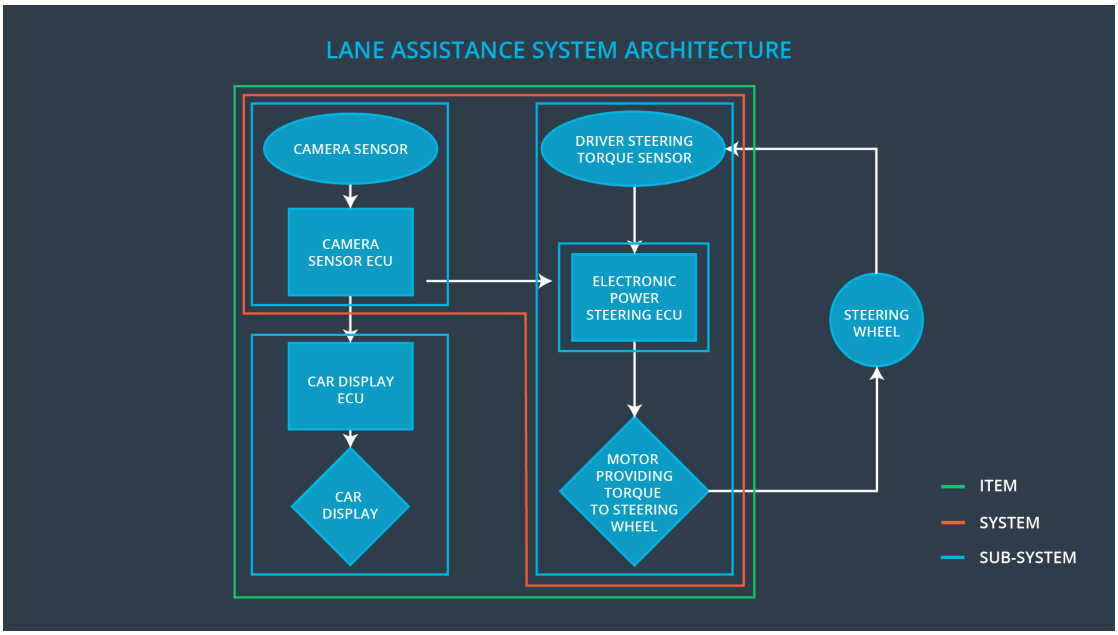

Figure 21: Preliminary architecture

Table 22: Architecture elements

Element	Descriptiion
Camera Sensor	provides Image to the Camera Sensor ECU
Camera Sensor ECU	performs image processing and identifies position of a vehicle w.r.t. the lane
Car Display	displays the status of the lane assistance item
Car Display ECU	accepts packet and displays on a car display if a lane assistance item malfunctions
Driver Steering Torque Sensor	senses the position of the steering wheel
Electronic Power Steering ECU	given current velocity, camera data, and steering wheel position determines whether more input is necessary
Motor	activates vibrations of the steering wheel

3 Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

3.1 Functional Safety Analysis

Table 31: Violations of the safety goals

Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting malfunction
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit)
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.

3.2 Functional Safety Requirements

Functional Safety Requirements for the Lane Departure Warning (LDW) are shown in Table 32.

Table 32: Functional Safety Requirements: Lane Departure Warning

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	the system is turned off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	the system is turned off

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria: are shown in Table 33.

Table 33: LDW Verification and Validation Acceptance Criteria

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	User study: driver's reaction to the Max_Torque_Amplitude while activating the item	Fault injection, model checking, formal analysis: meeting the requirement upon fault injection
Functional Safety Requirement 01-02	User study: driver's reaction to the Max_Torque_Frequency while activating the item	Fault injection, model checking, formal analysis: meeting the requirement upon injecting fault, performing model checking of the system

Functional Safety Requirements for the Lane Keeping Assistance (LKA) are shown in Table 34.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria: are shown in Table 35.

3.3 Refinement of the System Architecture

Figure 31 shows the refined architecture including all of the ASIL labels.

Table 34: Functional Safety Requirements: Lane Keeping Assistance

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	The lane keeping functionality is turned off

Table 35: LKA Verification and Validation Acceptance Criteria

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	User study: Max_Duration time interval in choosen in a way that drivers do not take their hands off the steering wheel	Verifying item functionality under fault injections

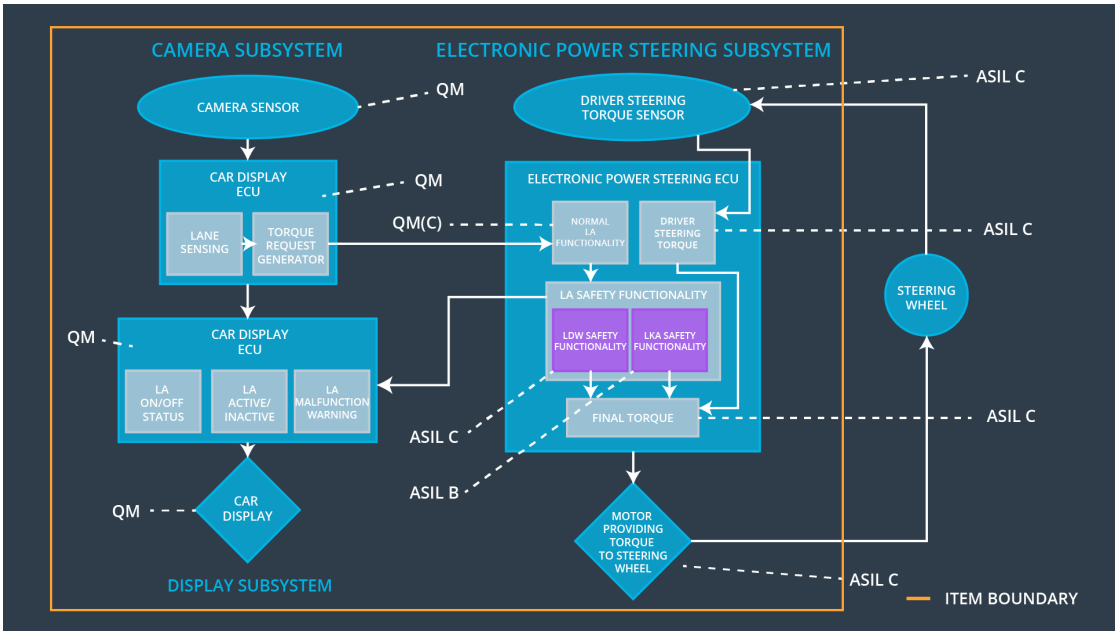

Figure 31: Refined architecture

3.4 Allocation of Functional Safety Requirements to Architecture Elements

Given the refined architecture presented in Figure 31 we allocate each functional safety requirement to a corresponding architecture element in Table 36.

Table 36: Mapping Functional Safety Requirements to Architecture

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	✓		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	✓		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	✓		

3.5 Warning and Degradation Concept

Table 37: Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Decreasing vibration torque	Vibration Torque frequency is above Max_Torque_Frequency and vibration torque amplitude is above Max_Torque_Amplitude	Yes	Indication light on car display on
WDC-02	Decreasing assistance torque	Lane keeing assistance is applied for more then Max_Duration time interval	Yes	Indication light on car display on

4 List of Abbreviations

ISO	International Organization for Standardization
ASIL	Automotive Safety Integrity Level
ECU	Electronic Control Unit
EPS	Electronic Power Steering
OEM	Original Equipment Manufacturer
LDW	Lane Departure Warning
LKA	Lane Keeping Assistance

Bibliography

[1] Organización Internacional de Normalización. *ISO 26262: Road Vehicles : Functional Safety*. ISO, 2011.